PROCESSING ACTIVITY MASKING IN A DATA PROCESSING SYSTEM

This invention relates to the field of data processing systems. More particularly, this invention relates to the masking of processing activity within data processing systems, for example, in order to increase security.

It is know to provide data processing systems which manipulate secure data and for which it is desirable to ensure a high degree of security. As an example, it is known to provide smart cards which include a data processing system which manipulates secure data, such as secret cryptographic keys, and this data must be kept secret in order to prevent fraud.

Known ways of attacking the security of such systems include timing analysis and power analysis. By observing the timing behaviour and/or the power consumption behaviour of such a system in response to inputs, information concerning the processing being performed and the data being manipulated can be determined in a way that can compromise security. It is strongly advantageous to provide resistance against such security attacks.

Viewed from one aspect the present invention provides apparatus for processing data under control of data processing instructions specifying data processing operations, said apparatus comprising:

a first execution mechanism operable to execute a first set of data processing instructions;

a second execution mechanism operable to execute a second set of data processing instructions, said first set of data processing instructions overlapping with said second set of data processing instructions such that one or more data processing instructions are executable by either said first execution mechanism or said second execution mechanism; and

an execution mechanism selector operable to pseudo randomly selected either said first execution mechanism or said second execution mechanism to execute one or more data processing instructions that are executable by either said first execution mechanism or said second execution mechanism.

The invention recognises that within a system having at least some instructions of an instruction set which may be executed by more than one execution mechanism, the power signature and other characteristics associated with those instructions can be

CLAIMS

1. Apparatus for processing data under control of data processing instructions specifying data processing operations, said apparatus comprising:

a first execution mechanism operable to execute a first set of data processing instructions;

a second execution mechanism operable to execute a second set of data processing instructions, said first set of data processing instructions overlapping with said second set of data processing instructions such that one or more data processing instructions are executable by either said first execution mechanism or said second execution mechanism; and

an execution mechanism selector operable to pseudo randomly selected either said first execution mechanism or said second execution mechanism to execute one or more data processing instructions that are executable by either said first execution mechanism or said second execution mechanism.

2. Apparatus as claimed in claim 1, wherein said first execution mechanism and said second execution mechanism have at least one different execution characteristic for at least one of said data processing instructions that are executable by either said first execution mechanism or said second execution mechanism.

3. Apparatus as claimed in claim 2, wherein said at least one different execution characteristic includes one or more of:

time to execute said data processing instruction; and

power consumption when executing said data processing instruction.

4. Apparatus as claimed in any one of claims 2 and 3, wherein at least one execution characteristic of at least one data processing instruction executed by one of said first execution mechanism or said second execution mechanism varies in dependence upon whether a preceding data processing instruction was executed with either said first execution mechanism or said second execution mechanism.

5. Apparatus as claimed in any one of the preceding claims, wherein all of said data processing instructions are executable by either said first execution mechanism or said second execution mechanism.

6. Apparatus as claimed in any one of the preceding claims, wherein said first execution mechanism is operable to execute some of said data processing instructions as native instructions directly controlling data processing hardware and remaining data processing instructions using emulation software.

7. Apparatus as claimed in any one of the preceding claims, wherein said second execution mechanism is operable to execute all of said data processing instructions using emulation software.

8. Apparatus as claimed in claims 6 and 7, wherein said first execution mechanism and said second execution mechanism share at least some emulation software.

9. Apparatus as claimed in any one of the preceding claims, wherein said data processing instructions are Java bytecode instructions.

10. Apparatus as claimed in claim 9, wherein said first execution mechanism includes native Java bytecode execution hardware and said second execution mechanism uses Java bytecode emulation for all Java bytecodes.

11. Apparatus as claimed in any one of the preceding claims, wherein said execution mechanism selector is controlled by a pseudo random execution mechanism selecting signal.

12. Apparatus as claimed in claim 11, comprising a processor core, said pseudo random execution mechanism selecting signal being an input to said processor core.

13. Apparatus as claimed in claim 12, wherein a pseudo random signal generator is operable to generate said pseudo random execution mechanism selecting signal.

14. Apparatus as claimed in any one of the preceding claims, wherein a system configuration parameter is operable to force said execution mechanism selector to select said first execution mechanism for all data processing instructions.

15. Apparatus as claimed in claim 14, wherein said system configuration parameter is stored in a system configuration register.

16. A method of processing data under control of data processing instructions specifying data processing operations, said method comprising the steps of:

executing a first set of data processing instructions with a first execution mechanism;

executing a second set of data processing instructions with a second execution mechanism, said first set of data processing instructions overlapping with said second set of data processing instructions such that one or more data processing instructions are executable by either said first execution mechanism or said second execution mechanism; and

pseudo randomly selecting with an execution mechanism selector either said first execution mechanism or said second execution mechanism to execute one or more data processing instructions that are executable by either said first execution mechanism or said second execution mechanism.

17. A method as claimed in claim 16, wherein said first execution mechanism and said second execution mechanism have at least one different execution characteristic for at least one of said data processing instructions that are executable by either said first execution mechanism or said second execution mechanism.

18. A method as claimed in claim 17, wherein said at least one different execution characteristic includes one or more of:

time to execute said data processing instruction; and

power consumption when executing said data processing instruction.

19. A method as claimed in any one of claims 17 and 18, wherein at least one execution characteristic of at least one data processing instruction executed by one of said first execution mechanism or said second execution mechanism varies in

dependence upon whether a preceding data processing instruction was executed with either said first execution mechanism or said second execution mechanism.

20. A method as claimed in any one of claims 16 to 19, wherein all of said data processing instructions are executable by either said first execution mechanism or said second execution mechanism.

21. A method as claimed in any one of claims 16 to 20, wherein said first execution mechanism is operable to execute some of said data processing instructions as native instructions directly controlling data processing hardware and remaining data processing instructions using emulation software.

22. A method as claimed in any one of claims 16 to 21, wherein said second execution mechanism is operable to execute all of said data processing instructions using emulation software.

23. A method as claimed in claims 21 and 22, wherein said first execution mechanism and said second execution mechanism share at least some emulation software.

24. A method as claimed in any one of claims 16 to 23, wherein said data processing instructions are Java bytecode instructions.

25. A method as claimed in claim 24, wherein said first execution mechanism includes native Java bytecode execution hardware and said second execution mechanism uses Java bytecode emulation for all Java bytecodes.

26. A method as claimed in any one of claims 16 to 25, wherein said execution mechanism selector is controlled by a pseudo random execution mechanism selecting signal.

27. A method as claimed in claim 26, comprising a processor core, said pseudo random execution mechanism selecting signal being an input to said processor core.

28. A method as claimed in claim 27, wherein a pseudo random signal generator is operable to generate said pseudo random execution mechanism selecting signal.

29. A method as claimed in any one of claims 16 to 28, wherein a system configuration parameter is operable to force said execution mechanism selector to select said first execution mechanism for all data processing instructions.

30. A method as claimed in claim 29, wherein said system configuration parameter is stored in a system configuration register.